MOC perspective: DTS versus FASTCopy
17 June 2004

The MOC team reevaluated DTS based on the user guide and discussions with Bob Schaefer and the DTS developers. We did not have time to install and evaluate the DTS software. Both DTS and FASTCopy meet the MOC's requirements for file transfer between the MOC and an external system. The GSSC had a few additional requirements that FASTCopy doesn't handle in the same way DTS does, but can be supported with additional software or procedures.

Although the new information corrected some misunderstanding of the capabilities of DTS, the MOC still prefers FASTCopy for file transfers to and from the MOC. The major reason is that FASTCopy is more secure than SSH file transfers used by DTS.

1. The MOC doesn't want external users to have access to the SSH port on our systems. There is no adequate way within open ssh to prevent an external user from copying files from where they are not supposed to. This is a key hole in our Swift design. FASTCopy does not use SSH.

2. We don't wan't to give external users system accounts to a MOC computer. As of this writing, nearly all major distributions of ssh servers require system accounts. SSH distributions that plug these holes probably cost more that FASTCopy alone. Although the risk can be plugged to some extent with decent null shells, it is still a risk for external users to have system accounts and passwords. FASTCopy does not use system accounts for external access. It is configurable with proxy accounts and passwords.

3. SSH's SCP and SFTP file access is not restrictable. An external user has all the read and write privileges granted to them of ANY file on the system that their system account has read and write privileges over. This is another key hole in our Swift design that I wish to plug. FASTCopy has additional directory and file restrictions that will allow us to restrict access to certain directories.

4. Its a given that we will not have sendmail access to the MOC. sendmail is notoriously buggy, vulnerable, and easily misconfigured. The NISN security folks normally require that I have all sendmail servers turned off. As noted by the DTS team, it is possible to have yet another piece of client software (fetchmail) poll external mail servers to retrieve mail. This adds yet another layer of complexity.

We are not saying that DTS itself is insecure. We just wish our system to be more secure than a system using any SSH-based file transfer. We want to move away from the inherent vulnerabilities of giving people ssh access to our systems. FASTCopy's proxy usernames and passwords meet this requirement.